# Perceived Control and Privacy in a Professional Cloud Environment

Michael Lang
Technical University of Munich
michael.lang@in.tum.de

Manuel Wiesche
Technical University of Munich
wiesche@in.tum.de

Helmut Krcmar
Technical University of Munich
krcmar@in.tum.de

## Abstract

*Cloud customers need to assess whether their cloud service provider offers high-quality services and handles sensitive information confidentially. Privacy protection is therefore a major challenge during cloud sourcing. Although cloud customers want control over their sensitive information, they have limited resources to do so. They therefore consider other control agents, such as certification authorities or collectives, but the effectiveness of these groups to ensure privacy protection is unknown. This study differentiates between three control agents (personal control, proxy control, and collective control) and investigates the influence of these agents on cloud customers' perceived control over sensitive information to protect privacy during cloud sourcing. Results show that proxy and collective control influence cloud customers' perceptions but personal control does not. Therefore, only external control agents, who can apply sanctions, are perceived as being able to effectively protect privacy.*

## 1. Introduction

Cloud computing is commonly used to gain on-demand network access to a shared pool of managed and scalable IT resources [4, 32]. The volume of sensitive information obtained (such as personal data) within this environment has increased exponentially, as an increasing number of companies considers personal data to be a corporate asset [40]. However, prior to the transfer of personal data or extending the use of sensitive information, companies need to assure customers that their cloud service provider has adequate security and privacy protections in place [14].

Cloud customers have limited means to assess as to which cloud service provider offers high-quality services and handles sensitive information in a confidential manner, and therefore, security and privacy concerns considerably restrict the adoption and expansion of cloud platforms [2, 16, 49].

Cloud customers are more likely to adopt cloud platforms if they are able to reduce their perceived privacy risks by ensuring that appropriate control exists over the sensitive information they provide [2]. However, they often have limited resources to adequately evaluate the security provided to protect their sensitive information in a cloud environment [39]. Simultaneously, customers desire certain outcomes, such as a positive relationship and privacy protection [17, 39]. In addition to personal control, proxy control (such as the certification of authorities) or collective control (as a member of a group to protect privacy) are often considered when selecting a cloud [15, 21]. These control agents can be differentiated with respect to their effectiveness in achieving the required amount of privacy protection [17], but such considerations are extremely challenging for cloud customers when selecting appropriate and effective control agents [15, 56].

In this study, we adopt a psychological control perspective to investigate the types of control agents that customers consider to be effective in protecting privacy in a cloud environment. More specifically, we adopt a psychological control theory that includes three control agents (personal control, proxy control, and collective control) and investigate the effect that these agents have on cloud customers' perceptions of privacy in a cloud environment. Using a survey study approach, we seek to answer the following research question: *What kind of control agents do cloud customers consider capable of protecting the privacy of their sensitive information?* Our findings highlight the importance of external control agents in influencing perceived privacy protection, and the intention that such agents have in expanding cloud services by the mediating effect of perceived control over sensitive information.

This paper describes the theoretical background relating to privacy as an inhibiting factor in adopting cloud services and discusses privacy control agents. On the basis of this theoretical background, we develop our hypotheses on the relationship between the differing control agents used to perceive control and to

URI: http://hdl.handle.net/10125/50352
ISBN: 978-0-9981331-1-9

protect privacy that customers have of such agents. Furthermore, we describe our research methodology and choice of operational construct, present intended theoretical and practical implications of our findings, and finally conclude the results of research.

## 2. Theoretical background and hypotheses

### 2.1 Privacy as a major inhibitor for cloud adoption and extension

Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" [32]. In this respect, computer resources refer to hardware, development platforms, and applications [5] that "can be rapidly provisioned and released with minimal management effort or service provider interaction" [32]. Cloud customers use these resources to process, transfer, and store sensitive information, such as personal data from customers, and to gain advantages with respect to costs and flexibility [32]. The receiving party (the cloud service provider) thus needs to have adequate privacy protection in place before cloud customers can feel safe about transferring sensitive information [14].

Security and privacy concerns serve as major inhibitors in adopting cloud and its subsequent expansion. Cloud customers have limited means to assess as to which cloud service provider offers high-quality services and can handle sensitive information in a confidential manner [2, 26, 49]. After selecting a cloud service provider, the customer transfers direct control of their sensitive information with no accurate knowledge of how exactly this provider will secure data and maintain associated confidentiality [2]. As a result, cloud customers perceive that they have a loss of control over their data, and they regard cloud computing as an uncertain environment [39]. To overcome these uncertainties, cloud customers seek mechanisms to assure and maintain control, such as certification of cloud services, privacy policies, or legal regulations [49, 64].

Cloud sourcing practices involve major management decisions, and it is important to understand the associated (cognitive) processes influencing the behavior of cloud customers [2]. In this respect, Benlian and Hess [2] investigated the sourcing opportunities of cloud sourcing and the risks facing decision makers. They concluded that cloud customers are more likely to increase cloud adoption, if they can reduce any perceived privacy risks through appropriate control over sensitive information.

In this study, we adopt a control perspective to clarify how cloud customers evaluate controls in place to ensure that their sensitive information and privacy are protected during cloud sourcing.

### 2.2 Privacy control in a cloud environment

Several behavioral scientists have emphasized the importance of control in relation to investigating privacy, where privacy is defined as an individual's ability to control the terms by which their sensitive information is acquired and used [35, 52, 55]. Therefore, privacy is viewed as "control over or regulation of, or more narrowly, limitations on or exemption from scrutiny, surveillance or unwanted access" [31]. According to Johnson [21], individuals use control to directly or indirectly attain privacy-related outcomes. In addition, individuals strive for control to motivate others to act in a way that is consistent with their privacy goals.

There are two research dimensions in control literature, which respectively focus on "what" control activities are used and "how" controls are enacted [56]. Prior studies have mainly focused on which control dimensions are used, and have shown that control activities are moderated by context factors, such as controller knowledge or boundary-spanning activities [23, 51]. The question as to how controls are enacted determines the effectiveness of control activities, and researchers have investigated the ability of the controller to align control activities with a current situation or in relation to past experiences [18, 38, 57]. This control dimension considers contrasting control styles (collaborative versus authoritative), both of which compete in complex situations [18], such as protecting privacy during cloud sourcing.

Individuals use direct or indirect controls to protect privacy in a cloud environment. The power and ability to influence others (controller) influences the use of a particular control style [56]. The cognitive and behavioral limitations of individuals often lead one to limiting oneself to a single style that fits best with the beliefs and skills of others [15]. To compete with a complex situation and benefit from different control styles, individuals conduct controls through not only themselves acting as a control agent (direct control) but also other control agents (indirect control) in order to control a desired outcome such as privacy protection [15, 21]. Both direct and indirect controls influence an individual's perceived control over a certain situation [12].

## 2.3 Types of control agents in cloud computing

Depending on the set priorities, a cloud customer chooses control agents that deliver a desired outcome [56]. However, control agents differ in their effectiveness with respect to reaching a desired outcome, such as enabling a positive relationship and protecting privacy [17]. While an individual cloud customer who acts as a control agent may prefer using collaborative control styles to protect his or her privacy and maintain a positive relationship with the cloud service provider, other control agents (such as certification authorities) instead rely on authoritative control styles that focus on privacy protection. This situation can be challenging for a cloud customer when searching for an effective control agent [15, 56].

In psychology, the construct of control has been treated as a perceptual construct because it is of greater interest than actual control when predicting behavior [44]. For example, perceived control has been identified as a powerful factor that influences an individual's risk perception and IT decision-making during IT projects [12]. The conceptualization of perceived control is therefore a cognitive construct, and as such it may be subjective [27]. Perceived control refers to an individual's beliefs regarding his or her ability to affect changes in the environment in a desired direction [8]. This study investigates the effectiveness of control agents based on cloud customers' perceived control over sensitive information.

On the basis of Yamaguchis' [63] work on the differentiation of control agents, we hypothesize that cloud customers are able to exercise personal control, proxy control, or collective control over their sensitive information to protect privacy (Table 1).

**Table 1. Control agents based on Yamaguchi [63]**

| Control agent | Controller | Privacy protection mechanism example |
|---|---|---|
| Personal control | Individuals | Monitoring, privacy policy |
| Proxy control | Powerful authorities | Certification, legislation |
| Collective control | Collective | Reputation |

**2.3.1 Personal control.** Individuals strive for primary control over their environment when they exercise personal control through individual self-protective actions [54]. Such a mechanism empowers cloud customers with direct control over the way in which sensitive information may be gathered by cloud service providers. Literature on privacy describes two major types of individual self-protection approaches [7, 25, 33, 46] - technological and non-technological control enactments.

Within an online environment (for example, in the context of cloud computing), users have the possibility of using privacy-enhancing technologies, such as user identification, authentication systems, or security features (for example, SSL connections or access management). As a result, cloud customers are able to configure an individual level of security to protect sensitive information [61].

Non-technological control enactments include mechanisms such as privacy policies provided by the cloud service provider [60]. In this regard, cloud customers can be informed about the choices available for the way cloud service providers use the information collected. However, technological control enactments are identified as being more powerful than non-technological control enactments [46], whereas non-technological control enactments have been identified as being capable of influencing the control perception of controllers within information systems [60, 61]. We therefore predict that personal control via privacy-enhancing technologies and privacy policies will enhance cloud customers' perceptions with respect to control over their information. Our hypothesis in this respect is as follows:

> *Hypothesis 1 (H1): Personal control mechanisms are a secondary outcome of privacy-enhancing technologies and privacy policies enhance cloud customers' perception of information control.*

**2.3.2 Proxy control.** Proxy control is an institution-based control mode wherein powerful authorities act as control agents [1]. With proxy control, individuals attempt to align themselves in order to be able to gain control through powerful others [61]. Normative rules about organizational behavior are defined and promulgated through active participation in a wide array of events, such as audits or legal investigations organized by certification authorities or government legislators [25, 26, 45]. Individuals believe that organizations subscribing to the professional publications of these associations learn acceptable norms of practices and affect the behavior of their organization accordingly [45]. In addition, it is believed that if organizations misbehave in terms of these norms, they will be punished by the powerful authorities [1]. Within a cloud context, cloud customers rely on certification authorities and governmental regulations to exercise proxy control over their sensitive information [39].

Third-party certification is defined as a "process in which a third-party formally confirms that a product, process or service conforms to a set of predefined criteria" (e.g., a certification scheme) [39]. These certifications provide independent verification of a provider's trustworthiness and its ability to protect

information. This independent verification is usually provided by knowledgeable and powerful authorities capable of enforcing external sanctions (for example, certificate termination) when cloud service providers are in breach of compliance with a certification scheme [34].

Some countries have established legislative efforts to protect sensitive information from unintended access and usage. The legal system, therefore, is a powerful control mechanism for the exercise of social control as it ensures that offenders are punished [25, 50] and thus deters potential offenders in the case of illegal behavior.

With respect to the deterrent effectiveness of certification authorities and legal systems, information systems studies have identified the positive effects of certificates and laws in the protection of sensitive information within an online environment [25, 29, 60]. Therefore, in this study, we predict that proxy control via third-party certification and an appropriate legal environment increases cloud customers' perception of information control. We therefore construct our second hypothesis as follows:

*Hypothesis 2 (H2): Proxy control mechanisms, as a secondary outcome of third-party certification and legislation, enhance cloud customers' perception regarding information control.*

**2.3.3 Collective control.** In collective control, an individual attempts to control the environment as a member of a group or collective, in which the group or the collective serve as an agent of control [1]. Collective control is implemented by promulgating common values, beliefs, and philosophies within the collective [23]. The collective propagates norms and values resulting in a group of individuals who share a common ideology, who have internalized a set of values, and who are committed to the collective [23]. If outsiders do not adhere to those norms, the collective control agent can sanction outsiders through informal mechanisms. In collective control, responsibility (as well as agency) is diffused among actors [28].

Collective controls have been identified as important collaborative control styles in situations when the individual is unable to observe the outsider's behavior [23, 56]. Within a cloud environment, cloud computing may be considered an uncertain environment in which transparency is limited [53]. In this respect, collective control styles are also important in an inter-organizational context.

Reputation is considered to play an important role in uncertain environments, where the information conveyed by reputation helps reduce social uncertainty among individuals [41]. Reputation, however, plays another role in reducing social uncertainty, where it often works as a sanction mechanism against dishonest deeds (e.g., reputation as hostage) [42]. Organizations may refrain from misconduct because they fear possible negative consequences with respect to their reputation [42, 62]. This sanctioning role of reputation is part of the mechanisms used to protect privacy; it directly reduces the incentive of the owner of the reputation to act dishonestly [25, 62].

In summary, the information aspect of reputation makes the recipient confident in adapting cloud services and revealing sensitive information. This leads to an enhancement of the consumer's perceived control over sensitive information. In this study, we therefore predict that collective control based on the reputation of the cloud service provider increases the cloud customers' perceived information control. Our hypothesis in this respect is as follows:

*Hypothesis 3 (H3): Collective control via reputation leads to increased cloud customers' perceived control over sensitive information.*

## 2.4 Information control and privacy

In accordance with previous research, we conceptualize information control as a perception and define it as being an individual's belief in the ability to determine the extent to which sensitive company information, such as personal data from customers, or private information will be released within a cloud environment in an unintended way [10]. Prior literature differentiates between two types of control important in a privacy context: control over information disclosure and control over information use once the information has been obtained [6, 47]. Most commonly, providers within the internet address the first dimension by offering granular privacy settings [19], which limit the accessibility of sensitive information to other members and third parties. However, it has been suggested that individuals feel they have a higher level of privacy when they have a sense of information control [7]. Recent studies on privacy suggest that a loss of information control is central to the perception toward privacy invasion [10].

Accordingly, in this study, we hypothesize that perceived information control is positively related to privacy, as follows:

*Hypothesis 4 (H4): Cloud customers' perceived information control positively affects privacy.*

## 2.5 Privacy and cloud customers' intention to expand cloud service

The theory of reasoned action asserts that attitudes toward behavior are generally accurate predictors of an individual's behavioral intention in an information

system environment [36]. Applying the theory of reasoned action to the cloud expansion context, we hypothesize that cloud service expansion intention is determined by a cloud customer's privacy. Privacy has an influential role in IT expansion and information disclosure behavior, and is supported at the individual and organizational level in different application contexts. For example, e-businesses will be used if customer privacy is protected [59]. At the organizational level, privacy has been found to be an important construct that enables online transactions and the transference of data to an external partner [14].

Therefore, in this study, we hypothesize that cloud customers' privacy is positively related to the expansion of the usage of cloud services, as follows:

> *Hypothesis 5 (H5): Cloud customers' privacy positively affects their intention to expand their use of cloud services.*

Figure 1 provides an overview of the hypotheses defined in our study.

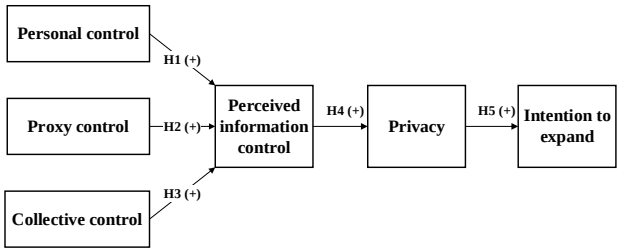


**Figure 1. Cloud privacy research model**

# 3. Methodology

## 3.1 Sample

To enable ease of design without sacrificing rigor, we implemented our research design within a professional cloud environment to match our target population [43]. We empirically tested our research hypotheses using the data collected through a survey that included items for the constructs specified in the model. The sample of our survey was drawn from a market research company, Digital Intelligence Institute (dii) between September and November 2016; dii is a leading research company studying digital developments within Germany.

To increase the external validity of our study, dii did not constrain the sample to specific industries or to firms of a specific size, and instead drew a random sample from the entire population of cloud decision makers within their database. The survey questionnaire was mailed to the most senior IT executive of each firm (e.g., to the chief information officer, the vice president in charge of IT, or the vice president in charge of business), along with a letter outlining the purpose of the research and soliciting participation.

## 3.2 Scale development

Scale development for the constructs (Table 2) was based on an extensive survey of literature on privacy and psychological control. We adapted validated standard scales and constructs for our use as far as possible. Table 2 provides the constructs used and a summary of the sources used to draw items for scales. All questions (except those regarding legislation) were answered using a Likert scale ranging from 1 to 5, with 1 representing the lowest score as "completely disagree" and 5 representing the highest score as "completely agree"; legislation questions were answered using a Likert scale ranging from 1 to 5 as well but with 1 representing the lowest score as "very low" and 5 representing the highest score as "very high" on the item scale.

Several control variables were added to control for the results affected by extraneous factors. These included participants' experience of cloud, the deployment model used by a specific cloud service, and whether personal data are processed within this specific cloud service.

To avoid potential language-barrier problems, the survey was provided in German. However, to check for translation bias within measurement items, a back-translation technique was employed wherein two different translators translated the German questionnaire back into English [3]. The back-translated items had a high degree of correspondence with the original English items, thereby assuring a relative lack of translation bias.

**Table 2. Construct operationalization**

| **Construct** | | **Source** |
|---|---|---|
| Intention to expand cloud services | | Benlian and Hess [2] |
| Privacy | | Dinev et al. [10] |
| Perceived information control | | Xu et al. [60] |
| Personal control | Privacy policy | Xu et al. [60] |
| | Privacy-enhancing technology | Hossain and Prybutok [20] |
| Proxy control | Legislation * | Koh et al. [24] |
| | Third-party certification | Kim et al. [22] |
| Collective control | Reputation | Doney and Cannon [11] |
| * Two additional self-developed constructs are considered to determine the influence of legislation.<br>In your opinion, how effective are the laws and regulations in the supplier's country concerning the following activities?<br>• Ensuring data privacy in the cloud.<br>• Ensuring data security in the cloud. | | |

### 3.3 Survey administration

The current study utilized a "key informants" methodology for data collection, which is a popular approach in empirical information systems studies [37]. In organizational survey research, targeted respondents assume the role of key informants and provide information on a particular unit of analysis by reporting on group or organizational properties. However, if a respondent lacks appropriate knowledge, the results can be confusing and may lead to erroneous conclusions. Therefore, it was important within the context of this study to identify respondents who were involved with and were most knowledgeable about cloud services. Consequently, we used a clear definition of cloud computing in the introduction to our survey.

We also indicated that the survey should be completed by the most senior executive available with a good overview of the organization's stance on cloud services. In addition, to increase the content validity of the responses and avoid social desirability bias, we asked respondents to complete the questionnaire with reference to one specific cloud service (e.g., CRM or storage) that they used or were familiar with.

To foster participation and reduce self-reporting bias, all participants were offered a report on their company's position compared with that of others of a similar size and industry. Finally, a pre-test assisted us in the development of both the content and the format of specific questions presented in the survey. Twenty practitioners from various industries known by dii evaluated the results, and we also employed two academics who are experts in cloud computing research.

In total, 109 usable responses (25% of the total customers with a cloud experience of more than three years, 38% with an experience of 1–3 years, and 37% with an experience of less than one year) were available for data analysis. The total sample included companies using cloud deployment models that were 55% public, 25% hybrid, and 20% private. In addition, 76% of the companies processed personal data within the cloud service, whereas 24% did not.

## 4. Data analysis and results

### 4.1 Measurement model

To assure validity of the constructs used, we adopted constructs used in previous studies. Our measurement model was validated using the standard procedure of Straub [48], and to assess the convergent and discriminant validity of items, the items of the scale were pooled into a related domain. While convergent validity was determined both at the individual indicator level and at the specified construct level, discriminant validity was assessed by analyzing the average variance extracted and inter-construct correlations.

Results showed that all the factor loadings were significant, suggesting convergent validity. All constructs met the threshold value for the average variance extracted (AVE > 0.50) and Cronbach's alpha (alpha > 0.70), as suggested by Straub [48]. For the discriminant validity of latent variables, the square roots of AVEs exceeded inter-construct correlations that were negligibly low between independent constructs. In addition, composite reliability (CR) was calculated and evaluated for each construct; all constructs were found to have a CR that was significantly above the cut-off value of 0.70. In summary, the quality of the measurement model was proven to be satisfactory.

Following the proscribed procedures of MacKenzie et al. [30], we also calculated the AVE for each second-order construct (personal control and proxy control) by averaging the square of each first-order sub-dimension's standardized loading on the second-order construct. All AVE values were found to exceed the threshold of 0.50, indicating that (on an average) the majority of the variance in first-order dimensions was shared with second-order constructs.

### 4.2 Structural model

We used SmartPLS 3.0 to validate the structural model and to test the hypotheses using the bootstrapping (1000 resamples) method. The second-order personal control and proxy control constructs were estimated using the factor scores of their first-order dimensions as reflective indicators (see Wright et al. [58]).

Our findings support most of the primary hypotheses of the study (H2, H3, H4, and H5). Proxy control ($\beta = 0.54$, $t = 6.34$) and collective control ($\beta = 0.27$, $t = 2.93$) are positively related to perceived information control and explain 47% of its variance. In turn, perceived control ($\beta = 0.66$, $t = 12.98$) is positively related to privacy and explains 44% of its variance. Finally, privacy ($\beta = 0.48$, $t = 5.40$) is positively related to the intention to expand cloud service with an explanation power of 23%. In contrast, the relationship between personal control ($t = 0.20$) and perceived information control is not significant at a 5% level, and therefore, H1 is not supported. However, none of the control variables significantly affect perceived control or privacy. Figure 2 illustrates the final results obtained from the research model.

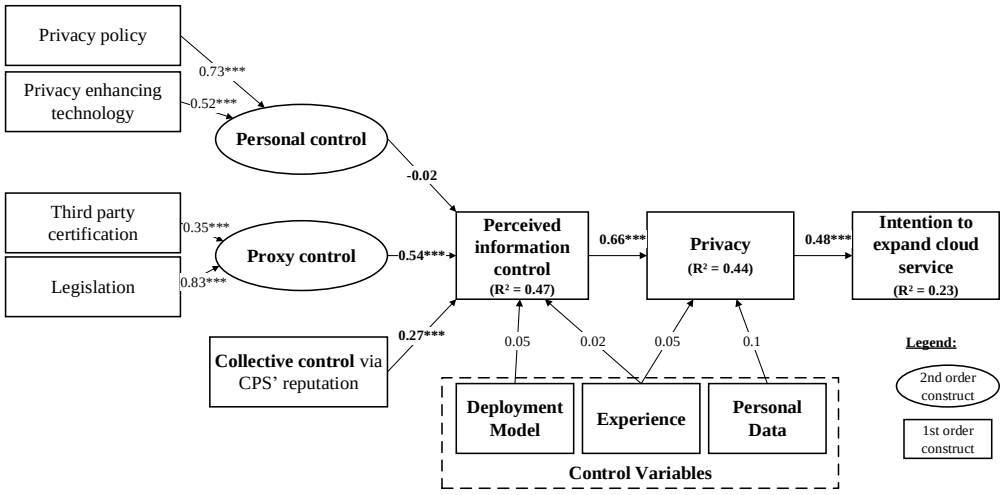


**Figure 2. Cloud privacy research model results**

### 4.3 Mediation test

In our theoretical model, we posited that perceived information control would mediate the relationship between control agents and privacy. To test this mediation, we conducted a Sobel test, which is a method for assessing indirect affects, and is considered superior (e.g., it provides a better balance between Type I and Type II errors) to the traditional Baron-Kenny mediation test [9]. We then conducted the Sobel test for the indirect effects of proxy control and collective control on privacy through perceived information control using Preacher's online Sobel test calculator (http://quantpsy.org/sobel/sobel.htm). The Sobel test statistics were significant for (i) the relationship between proxy control and privacy ($z = 5.54$; $p < 0.001$) and (ii) the relationship between collective control and privacy ($z = 4.78$; $p < 0.001$), thereby suggesting that perceived information control plays a mediating role between control agents and privacy.

## 5. Discussion, implications, and limitations

### 5.1 Discussion

Results of this study provide insights into effective control agents operating within a cloud environment. This study differentiates between three control agents (personal control, proxy control, and collective control), and investigates their influences on cloud customers' perceived control over sensitive information and privacy during cloud sourcing.

Although proxy and collective control influence cloud customers, we identified no support from the customers used in our sample for personal control. Hence, only external control agents, which are known to be able to apply sanctions, are perceived to be effective. Furthermore, this study identified the mediation effects of perceived information control between control agents and privacy.

### 5.2 Implications

Our findings have important implications for theory and practice. First, we have extended available literature on privacy by identifying perceived information control as a mediator between control agents and privacy within a professional cloud environment. Research on privacy has previously been conducted mainly within a consumer context [10], although professionals also struggle with privacy issues [14]. Our findings provide evidence of the importance of privacy within a professional context and demonstrate the importance of considering the mediating effects of control perception when investigating privacy protection through different control agents and the privacy protection mechanisms used.

Second, we analyze cloud sourcing decision-making by investigating how individuals' perception of control and privacy influences their purchasing decisions [25]. We demonstrate how cloud customers control sensitive information and ensure privacy within a cloud environment. Such findings are vital for cloud research because they show how different actors influence the cloud sourcing decisions made by cloud customers.

Third, our results extend literature on control by considering different control agents. In line with

Gregory and Keil [15], we argue that although different control agents are important, the differences between their effectiveness should be considered. Furthermore, many studies focus on the perspective of the controlee and investigate if the controlee perceives that the enacted controls are appropriate [18, 38, 51]. We extend this view by investigating the control perception of a controller with respect to the effectiveness of the controls enacted through control agents. According to our findings, even if controllers have limited resources to control others, additional means of control are available by considering external control agents. Hence, we extend the known literature on control by providing a third dimension "who controls?" which should be considered when investigating enacted controls.

This research also has managerial implications. Our findings contribute to the knowledge used by cloud customers, cloud service providers, legislative and certification authorities, and the society as a whole, by determining effective control agents that influence decision-making in a cloud environment.

Our results assist cloud customers in identifying appropriate controls to assure that a cloud service provider has adequate security and privacy protection in place. For cloud service providers, our results indicate as to which mechanisms are appropriate for use in protecting privacy from a customers' perspective. Our findings also provide governments, certification authorities, and the society with feedback on the effectiveness of their endorsements. It is considered that these groups might use our results to improve their services and employ reliable and reputable certification authorities, or to consider further channels to share opinions and information on the reputation of cloud service providers.

### 5.3 Limitations

This study was conducted in Germany. Therefore, researchers have to be careful when attempting to generalize the results to other social, economic, legal and cultural environments. Privacy is a relative concept and may be related to cultural values [22]; what is considered private in one culture or legal region may not be considered private in another. For example, people in the U.S. tend to take a "privacy pragmatist" perspective, whereas Europeans (including Germans) are concerned about their privacy and are more likely to take the perspective of "privacy fundamentalists" [13].

Furthermore, we acknowledge that other critical factors are relevant, such as the strategic importance of cloud services, the home country of a cloud customer, or how trust affects cloud customers privacy perception and expansion decisions. However, our results show that privacy influences the decisions made by cloud customers when extending cloud services, and therefore demonstrates important insights into how cloud expansion decisions are made.

## 6. Conclusion

Results of this study provide insights on effective control agents within a cloud environment. We found that cloud customers seek control over sensitive information through external control agents, such as institutions, governments, or the society, who are able to apply sanctions.

From a theoretical point of view, our research identifies perceived information control as a mediator between control agents and privacy. This research extends the existing literature on control by identifying a third dimension, which considers external control agents in addition to the controller. Our findings illuminate the way in which control agents influence cloud customers during decision-making. From a managerial point of view, our study contributes to a better understanding of effective control agents acted within a cloud environment.

## 7. Acknowledgments

This research is a part of the research project, Next Generation Certification (NGCert) (www.ngcert.eu), and was funded by the German Federal Ministry for Education and Research (grant. No. 16KIS0078). The authors would like to thank dii and Wilfried Heinrich for supporting the data collection process.

## 8. References

[1] A. Bandura, "Social Cognitive Theory: An Agentic Perspective", Annual Review of Psychology, 2001, pp. 1-26.

[2] A. Benlian and T. Hess, "Opportunities and Risks of Software-as-a-Service: Findings from a Survey of It Executives", Decision Support Systems, 2011, pp. 232-246.

[3] A. Bhattacherjee and S.C. Park, "Why End-Users Move to the Cloud: A Migration-Theoretic Analysis", European Journal of Information Systems, 2014, pp. 357-372.

[4] M. Böhm, et al., "Towards a Generic Value Network for Cloud Computing, in International Workshop on Grid Economics and Business Models", Springer, Berlin Heidelberg, 2010, pp. 129-140.

[5] M. Böhm, et al., "Cloud Computing: Outsourcing 2.0 Oder Ein Neues Geschäftsmodell Zur Bereitstellung Von It-Ressourcen", Information Management & Consulting, 2009, pp. 6-14.

[6] M.J. Culnan and P.K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", Organization Science, 1999, pp. 104-115.

[7] M.J. Culnan and R.J. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations", Journal of Social Issues, 2003. 59(2): pp. 323-342.

[8] R. De Charms, Personal Causation: The Internal Affective Determinants of Behavior, Routledge, New York, 2013.

[9] J.R. Detert, L.K. Treviño, and V.L. Sweitzer, "Moral Disengagement in Ethical Decision Making: A Study of Antecedents and Outcomes", Journal of Applied Psychology, 2008, pp. 374-391.

[10] T. Dinev, et al., "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts", European Journal of Information Systems, 2013, pp. 295-316.

[11] P.M. Doney and J.P. Cannon, "An Examination of the Nature of Trust in Buyer-Seller Relationships", Journal of Marketing, 1997, pp. 35-51.

[12] S. Du, et al., "Attention-Shaping Tools, Expertise, and Perceived Control in It Project Risk Assessment", Decision Support Systems, 2007, pp. 269-283.

[13] H. Galanxhi and F.F.H. Nah, "Privacy Issues in the Era of Ubiquitous Commerce", Electronic Markets, 2006, pp. 222-232.

[14] S. Goodman, "Protecting Privacy in a B2b World", Mortgage Banking, 2000, pp. 83-87.

[15] R.W. Gregory and M. Keil, "Blending Bureaucratic and Collaborative Management Styles to Achieve Control Ambidexterity in Is Projects", European Journal of Information Systems, 2014, pp. 343-356.

[16] P. Heidkamp and A. Pols, Cloud-Monitor 2017, in Cloud-Computing in Deutschland - Status quo und Perspektiven. 2017, KPMG AG: Bitkom.

[17] J.C. Henderson and S. Lee, "Managing I/S Design Teams: A Control Theories Perspective", Management Science, 1992, pp. 757-777.

[18] J. Heumann, et al., "To Coerce or to Enable? Exercising Formal Control in a Large Information Systems Project", Journal of Information Technology, 2015, pp. 337-351.

[19] C.M. Hoadley, et al., "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry", Electronic Commerce Research and Applications, 2010, pp. 50-60.

[20] M.M. Hossain and V.R. "Prybutok, Consumer Acceptance of Rfid Technology: An Exploratory Study", IEEE Transactions on Engineering Management, 2008, pp. 316-328.

[21] C.A. Johnson, Privacy as Personal Control. Man-Environment Interactions: Evaluations and Applications, ed. D.H.C.e. Part 2, Environmental Design Research Association, Washington, DC, 1974.

[22] D.J. Kim, et al., "Web Assurance Seal Services, Trust and Consumers' Concerns: An Investigation of E-Commerce Transaction Intentions across Two Nations", European Journal of Information Systems, 2015, pp. 252-273.

[23] L.S. Kirsch, "Portfolios of Control Modes and Is Project Management", Information Systems Research, 1997, pp. 215-239.

[24] T.K. Koh, M. "Fichman, and R.E. Kraut, Trust across Borders: Buyer-Supplier Trust in Global Business-to-Business E-Commerce", Journal of the Association for Information Systems, 2012, pp. 886-922.

[25] M. Lang, M. Wiesche, and H. Krcmar, Conceptualization of Relational Assurance Mechanisms - a Literature Review on Relational Assurance Mechanisms, Their Antecedents and Effects, in International Conference on Wirtschaftsinformatik. 2017: St. Gallen.

[26] M. Lang, M. Wiesche, and H. Krcmar, What Are the Most Important Criteria for Cloud Service Provider Selection? A Delphi Study, in European Conference on Information Systems. 2016: Istanbul.

[27] E.J. Langer, "The Illusion of Control", Journal of Personality and Social Psychology, 1975, pp. 311.

[28] B. Latané and J.M. Darley, The Unresponsive Bystander: Why Doesn't He Help? 1970, New York: Prentice Hall.

[29] P.B. Lowry, et al., "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers", Journal of the American Society for Information Science and Technology, 2013, pp. 755-776.

[30] S.B. MacKenzie, P.M. Podsakoff, and N.P. Podsakoff, "Construct Measurement and Validation Procedures in Mis and Behavioral Research: Integrating New and Existing Techniques", Management Information Systems Quarterly, 2011, pp. 293-334.

[31] S.T. Margulis, "Privacy as a Social Issue and Behavioral Concept", Journal of Social Issues, 2003, pp. 243-261.

[32] P. Mell and T. Grance, The Nist Definition of Cloud Computing. 2011, National Institute of Standards and Technology.

[33] G.R. Milne and M.J. Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices", Journal of Interactive Marketing, 2004, pp. 15-29.

[34] K. Oezpolat, et al., "The Value of Third-Party Assurance Seals in Online Retailing: An Empirical Investigation", Information Systems Research, 2013, pp. 1100-1111.

[35] P.A. Pavlou, "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?",

Management Information Systems Quarterly, 2011, pp. 977-988.

[36] P.A. Pavlou and M. Fygenson, "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior", Management Information Systems Quarterly, 2006, pp. 115-143.

[37] A. Pinsonneault and K. Kraemer, "Survey Research Methodology in Management Information Systems: An Assessment", Journal of Management Information Systems, 1993, pp. 75-105.

[38] U. Remus, et al. Control Modes Versus Control Styles: Investigating Isd Project Control Effects at the Individual Level. in International Conference on Information Systems. 2016. Dublin.

[39] S. Schneider and A. Sunyaev, "Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the It Outsourcing Literature in the Era of Cloud Computing", Journal of Information Technology, 2016, pp. 1-31.

[40] P.M. Schwartz, "Property, Privacy, and Personal Data", Harvard Law Review, 2004, pp. 2056-2128.

[41] A. Schwarz, et al., "A Conjoint Approach to Understanding It Application Services Outsourcing", Journal of the Association for Information Systems, 2009, pp. 748-781.

[42] D.L. Shapiro, B.H. Sheppard, and L. Cheraskin, "Business on a Handshake", Negotiation Journal, 1992, pp. 365-377.

[43] M. Siponen and A. Vance, "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations", European Journal of Information Systems, 2014, pp. 289-305.

[44] E.A. Skinner, "A Guide to Constructs of Control", Journal of Personality and Social Psychology, 1996, pp. 549-570.

[45] J.-Y. Son and I. Benbasat, "Organizational Buyers' Adoption and Use of B2b Electronic Marketplaces: Efficiency-and Legitimacy-Oriented Perspectives", Journal of Management Information Systems, 2007, pp. 55-99.

[46] J.-Y. Son and S.S. Kim, "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model", Management Information Systems Quarterly, 2008, pp. 503-529.

[47] S. Spiekermann. Perceived Control: Scales for Privacy in Ubiquitous Computing. in International Conference on User Modeling. 2005. Edinburgh.

[48] D.W. Straub, "Validating Instruments in Mis Research", Management Information Systems Quarterly, 1989, pp. 147-169.

[49] A. Sunyaev and S. Schneider, "Cloud Services Certification", Communications of the ACM, 2013, pp. 33-36.

[50] C.R. Tittle, Sanctions and Social Deviance: The Question of Deterrence, Praeger, New York, 1980.

[51] A. Tiwana and M. Keil, "Control in Internal and Outsourced Software Projects", Journal of Management Information Systems, 2009, pp. 9-44.

[52] S.D. Warren and L.D. Brandeis, "The Right to Privacy", Harvard Law Review, 1890, pp. 193-220.

[53] C. Weinhardt, et al., "Cloud Computing – a Classification, Business Models, and Research Directions", Business & Information Systems Engineering, 2009, pp. 391-399.

[54] J.R. Weisz, F.M. Rothbaum, and T.C. Blackburn, "Standing out and Standing In: The Psychology of Control in America and Japan. American Psychologist, 1984, pp. 955-969.

[55] A.F. Westin, "Privacy and Freedom", Washington and Lee Law Review, 1968, pp. 166-170.

[56] M. Wiener, et al., "Control Configuration and Control Enactment in Information Systems Projects: Review and Expanded Theoretical Framework", Management Information Systems Quarterly, 2016, pp. 741-774.

[57] M. Wiesche, M. Schermann, and H. Krcmar, Understanding the Enabling Design of It Risk Management Processes, in International Conference on Information Systems. 2015: Fort Worth.

[58] R.T. Wright, et al., "Operationalizing Multidimensional Constructs in Structural Equation Modeling: Recommendations for Is Research", Communications of the Association for Information Systems, 2012, pp. 367-412.

[59] H. Xu, R.E. Crossler, and F. BéLanger, "A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers", Decision Support Systems, 2012, pp. 424-433.

[60] H. Xu, et al., "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances", Journal of the Association for Information Systems, 2011, pp. 798-824.

[61] H. Xu, et al., "Research Note - Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services", Information Systems Research, 2012, pp. 1342-1363.

[62] T. Yamagishi and M. Yamagishi, "Trust and Commitment in the United States and Japan", Motivation and Emotion, 1994, pp. 129-166.

[63] S. Yamaguchi, Culture and Control Orientations. The Handbook of Culture and Psychology, Oxford University Press, New York, 2001.

[64] H. Yang and M. Tate, "A Descriptive Literature Review and Classification of Cloud Computing Research", Communications of the Association for Information Systems, 2012, pp. 35-60.